Basic *Children's Internet Protection Act* (CIPA)

REQUIREMENTS

Stage 1 **ONLINE SAFETY REQUIREMENTS**

Grades 4-5

Children's Internet Protection Act

Background

The Children's Internet Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011.

What CIPA Requires

Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measure must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must **provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.**

Federal Communications Commission
445 12th Street SW, Washington, DC 20554
Phone: 1-888-225-5322

TABLE OF CONTENTS

Basic *Children's Internet Protection Act* (CIPA) Implementation Guide

Common Sense Media's free, comprehensive E-rate Toolkit at www.commonsense.org/erate provides you, your teachers, and your school community with all of the resources you need to educate your students about three CIPA-required topics: 1) appropriate online behavior, 2) safety and privacy, and 3) cyberbullying. The Toolkit contains lessons organized by grade, complete with supporting student handouts, videos, assessments, and parent tips, as well as a Teacher Verification Document.

ELEMENTARY SCHOOL

One 45-minute lesson per grade per year

Grade	Lesson
K	Going Places Safely
1	Sending Email
2	Show Respect Online
3	Follow the Digital Trail
4	The Power of Words
5	Talking Safely Online

MIDDLE SCHOOL

Two 45-minute lesson per grade per year

Grade	Lesson
6	• Safe Online Talk • Strong Passwords
7	• Trillion Dollar Footprint • Cyberbullying: Crossing the Line
8	• Which Me Should I Be? • Cyberbullying; Be Upstanding

Access these lessons from the Toolkit's Teacher Page: www.commonsense.org/erate-teachers.

www.commonsense.org

E-RATE TOOLKIT

Teacher Verification Document

common sense media

TEACHER NAME: _____

TITLE: _____

GRADE/CLASS: _____

SCHOOL: _____

DISTRICT: _____

SCHOOL YEAR: _____

I verify that I have...

❒ Understood and embraced the district-wide Internet Safety Policy and the education requirements related to Children's Internet Protection Act (CIPA).

❒ Educated my students according to the lesson requirements.

I hereby certify that the above actions have been carried out during the 20___ – 20___ school year.

SIGNATURE: _____ **DATE:** _____

Teacher, please sign and turn in this Teacher Verification Document and any other pertinent paperwork required by your district.

ACCEPTABLE USE AGREEMENT

English

Spanish

BAKERSFIELD CITY SCHOOL DISTRICT
1300 Baker Street
Bakersfield, CA 93305

ACCEPTABLE USE AGREEMENT (AUA): DISTRICT TECHNOLOGICAL RESOURCES

Background Information, Commitments, and General Requirements

The Governing Board of the Bakersfield City School District's ("District") has adopted a policy (Student Use of Technology, BP 400.43) describing rules and procedures to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of, or access to, sensitive information, and to comply with the: (1) Children's Online Privacy Protection Act (15 USC 6501-6506 & 47 CFR 312.1-312.12); (2) Broadband Data Improvement Act. (Pub.L. 110-385.); (3) Protecting Children in the 21st Century Act (15 USC 6551); (4) Children's Internet Protection Act (20 USC 6301 et seq); (5) Enhancing Education Through Technology Act of 2001 (20 USC 6751 et seq.); and (6) the internet safety provisions of the No Child Left Behind Act (20 USC 6777). This *Acceptable Use Agreement* (*AUA*) brings together information from several District policies describing user obligations and responsibilities. The term "user" means anyone using District technological resources (e.g., computers, Internet, email, other forms of direct electronic communications, and equipment provided by the District regardless of the physical location of the user).

The District will use technology protection measures to block or filter, to the extent possible, access of visual depictions that are *obscene, pornographic, and harmful to minors* over the network. The District reserves the right to monitor use of the District's technology resources for improper use without advance notice or consent and to take immediate corrective action regarding any improper activities. As the District deems necessary, authorized employees will: (1) monitor users' online activities; (2) access, review, and copy; (3) store or delete any electronic communication or files; and (4) disclose files and documents to others. Users have no expectation of privacy regarding their use of District technological resources.

Users shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on race or ethnicity, ethnic group identification, physical or mental disability, medical condition, marital or parental status, sex or gender, gender identity, gender expression, genetic information, age, color, ancestry, national origin or nationality, religion, limited proficiency in English, or sexual orientation.

District staff will provide age-appropriate instruction to students about the safe, proper, and appropriate behavior while using technological resources. Although student use of District technological resources to access public social networking sites is prohibited, such instruction shall include, but not be limited to: the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, interacting with other individuals on social networking web sites and in chat rooms, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

Use of District Technological Resources

Before a student is authorized to use the District's technological resources, the student and his/her parent/guardian shall sign and return this *AUA* to acknowledge and agree to all the conditions specified here. Each District school will keep a copy of the *AUA* signature page on file. Annually and before each student uses District technology, the principal/designee will verify the presence of a fully executed *AUA*. Once signed, the *AUA* acknowledgement/permission page remains in effect until: (1) revoked by the parent; (2) the student has a cancellation of user privileges; or (3) the student is no longer enrolled. Even without a signature on the *AUA*, employees, students, and all other users are required to follow applicable laws, policies, procedures, including

the requirements described within this *AUA*. By using the District resources, each user agrees to comply with all rules. Each user is required to report any misuse of the District's technological resources to the appropriate employee (e.g., teacher, supervisor, or other District personnel). If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a teacher, supervisor, or other appropriate District personnel.

Students are authorized to use District technological resources or equipment to access the Internet or other online services in accordance with Board policy, the user obligations, and responsibilities specified in the District's *Acceptable Use Agreement*.

Accessing Technological Resources Outside of School Setting. Students will access the District technological resources outside of school only if a parent or legal guardian supervises their usage at all times. The student's parent or guardian is responsible for monitoring the minor's use outside of school.

Penalties for Improper Use

Students who violate District or school rules and regulations, to include the unacceptable uses of the District's technological resources may be subject to consequences including, but not limited to: (1) legal action; (2) suspension; (3) expulsion; (3) transfer to alternative programs; (4) cancelling or limiting student user privileges; (5) denial of participation in extracurricular or cocurricular activities; (6) or other privileges. When a crime may have been committed, the Superintendent or designee shall notify local law enforcement. In accordance with law and policy, students also may be subject to a District or school consequence(s), for any off-campus conduct during non-school hours that poses a threat or danger to the safety of students, staff, or District property, or substantially disrupts school activities.

Disclaimer

The District makes no guarantees and denies any responsibility for the accuracy or quality of the information obtained by using District technological resources. Any statement accessible through the District's resources is understood to be the author's individual point of view and not that of the District, its affiliates, or employees. The student and parent/guardian, as a condition of the student's use of District technological resources, agree to indemnify and hold harmless the District or any District employee and waive all claims or suits for damages, costs, or injury arising from the failure of any technology protection measures, violations of copyright restrictions, user mistakes or negligence, or other obligations arising from use of District technological resources. Any charges a user accrues due to the inappropriate and unauthorized use of the District's resources are to be borne by the user.

BAKERSFIELD CITY SCHOOL DISTRICT:
ACCEPTABLE USE AGREEMENT
ADDITIONAL STUDENT AGREEMENTS

Personal Responsibility and Safety

1. I will use the school computers safely, responsibly, and for educational purposes.
2. I will take care of the computer and all technology equipment as if it belonged to me.
3. I will keep my passwords private and not share them with my friends.
4. I will only use school computers for classroom work assigned by the teacher.
5. I will report any misuse of the computer or the network to a teacher or the principal.
6. I will immediately stop and tell the teacher or person in charge if anything happens on the computer or on the Internet that is wrong or makes me feel uncomfortable.

Inappropriate Uses

7. I will not use someone else's username and password to log into the computer or network.
8. I will not read, delete, copy, or modify email or use another person's identity.
9. I will not attempt to bypass security measures on the District network.
10. I will not download any software from the Internet unless specifically directed to as part of a lesson.
11. I will not buy, sell, or advertise anything using the school computer and/or network.
12. I will not use technology equipment to encourage the use of drugs, alcohol, and tobacco or take any action that is unethical or prohibited by law or District policy.

Digital Citizenship

13. I will not threaten, harass, insult, ridicule, gossip, or tease others while I am online or using a computer. I understand these behaviors may result in punishment to include loss of privileges.
14. I will not copy information and use it as if it were my own ideas without giving credit to the information's author and source. I know that failure to properly cite my sources of information is called plagiarism and is a form of cheating.

Online Behavior

15. I understand that computer files and electronic communications are not private and may be accessed by the District to ensure proper use.
16. I will not share personal information (either my own nor another student's) including: references to where I live, details about family or friends (including names), my age, birthday, home address, or telephone number on the Internet.
17. I will use respectful and appropriate language without swearing, name calling, or causing others to feel uncomfortable due to their gender, race, appearance, behavior, or beliefs. (These are actions that could be considered harassment or bullying).
18. I will not post copyrighted material online.

Required Signatures: BCSD *Acceptable Use Agreement*

STUDENT

By signing below, I am showing I understand and agree to follow all rules listed in this four-page *Acceptable Use Agreement*. I understand that any rules I do not follow may result in disciplinary action, losing my user account, and legal action. I further understand I may be held responsible for using technological resources outside of school if my conduct violates District rules. I agree to report any misuse of the District electronic system to a teacher, principal, or other District employee.

Student Name (please print):_____

Student Signature_____ Date_____

PARENT OR GUARDIAN

As the parent/guardian of this student, I have read and understand this *Acceptable Use Agreement* (*AUA*) consisting of four pages. I understand this *AUA* has been designed to help ensure safe, proper, and appropriate conduct while staff and students use technological resources. By signing below, I am consenting to my student using District technological resources consistent with all the provisions of this *AUA*. I further understand I may revoke this consent in writing, but this revocation will not affect any action taken in reliance on my consent before the District receives my written notice of revocation.

Parent or Guardian Name (please print):_____

Signature_____ Date_____

SPONSORING TEACHER

I have received and read Board Policy 400.43 entitled Student Use of Technology, the accompanying administrative regulation, and this *Acceptable Use Agreement* (*AUA*) describing expectations for the appropriate use of the District's technological resources. I have been provided with information about the role of staff to supervise student use of technological resources. As the sponsoring teacher, I agree to instruct the student to fulfill the requirements of the policy and *AUA*. This commitment includes agreeing to report any prohibited use or misuse of the District's technological resources to the appropriate Bakersfield City School District administrator and to comply with all applicable law, policy, and procedure.

Teacher's Name (please print):_____

Signature_____ Date_____

BAKERSFIELD CITY SCHOOL DISTRICT
1300 Baker Street
Bakersfield, CA 93305

ACUERDO DEL USO ACEPTABLE (AUA): RECURSOS TECNOLÓGICOS DEL DISTRITO

Información de los antecedentes, compromisos, y requisitos generales

La mesa directiva gobernante del Distrito Escolar de la Ciudad de Bakersfield ("Distrito") ha adoptado una norma (Uso de tecnología del estudiante, BP 400.43) describiendo las reglas y procedimientos para prevenir el acceso no autorizado y otras actividades ilícitas por usuarios en línea, prevenir la divulgación no autorizada, acceso, información sensitiva, y para cumplir con: (1) Decreto de Protección de la Privacidad En Línea de los Niños (15 USC 6501-6506 & 47 CFR 312.1-312.12); (2) Decreto del Mejoramiento de Datos de Banda Ancha. (Pub.L. 110-385.); (3) Decreto Protegiendo a los Niños en el Siglo XXI (15 USC 6551); (4) Decreto de Protección de Internet de los Niños (20 USC 6301 et seq); (5) Decreto de Mejoramiento de la Educación Por Medio de la Tecnología del 2001 (20 USC 6751 et seq.); y (6) y las provisiones de seguridad del Internet del Decreto Ningún Niño se Quedará Atrás (20 USC 6777). Este *acuerdo del uso Aceptable* (*AUA*) une la información de varias normas del distrito describiendo las obligaciones y responsabilidades del usuario. El término "usuario" significa cualquier persona usando los recursos tecnológicos del distrito (ej., computadoras, Internet, correo electrónico, otras formas de comunicaciones electrónicas directas, y equipo proveído por el distrito a pesar de la ubicación física del usuario).

El distrito usará medidas de protección de tecnología para bloquear o filtrar, hasta el punto posible, acceso de descripciones visuales que son *obscenas, pornográficas, y dañinas para los menores* en la red informática. El distrito reserva el derecho de monitorear el uso de los recursos de tecnología del distrito por uso impropio sin aviso de anticipo o consentimiento y tomar una acción correctiva inmediata respecto a cualquier actividad impropia. Como el distrito considere necesario, los empleados autorizados: (1) monitorearán las actividades en línea de los usuarios; (2) conseguirán acceso, revisarán, y copiarán; (3) almacenarán o borrarán cualquier comunicación electrónica o archivos; y (4) divulgarán archivos y documentos a otros. Los usuarios no tienen expectación de privacidad respecto a su uso de recursos tecnológicos del distrito.

Los usuarios no deberán conseguir acceso, anunciar, someter, publicar, o mostrar cuestiones dañinas o inapropiadas que sean amenazadoras, obscenas, perturbadoras, o sexualmente explícitas, o que podrían ser interpretadas como acoso o menosprecio de los demás basado en la raza o etnicidad, identificación de grupo étnico, discapacidad mental o física, condición médica, estado civil o paternal, sexo o género, identidad de género, expresión de género, información genética, edad, color, ascendencia, origen nacional o nacionalidad, religión, aptitud limitada en inglés, u orientación sexual.

El personal del distrito proveerá instrucción de edad apropiada a los estudiantes acerca del comportamiento seguro, propio y apropiado mientras usan los recursos tecnológicos. Aunque el uso de los recursos tecnológicos del distrito del estudiante para conseguir acceso a sitios de redes sociales públicos es prohibido, tal instrucción deberá incluir, pero no estará limitada a: los peligros de anunciar información personal en línea, mala representación por depredadores en línea, cómo reportar amenazas o contenido inapropiado u ofensivo, interactuar con otros individuos en sitios de redes sociales y salas de charlas, comportamientos que constituyen acoso cibernético, y cómo responder cuando se es sujetado al acoso cibernético.

Uso de los recursos tecnológicos del distrito

Antes de que un estudiante sea autorizado para usar los recursos tecnológicos del distrito, el estudiante y su padre/madre/tutor deberá firmar y regresar este Acuerdo del uso aceptable (*AUA)* para reconocer y estar de acuerdo a todas las condiciones especificadas aquí. Cada escuela del distrito mantendrá una copia de la página

de la firma del *AUA* archivada. Anualmente y antes de que un estudiante use la tecnología del distrito, el director/designado verificará la presencia de un *AUA* totalmente ejecutado. Una vez firmada, la página de reconocimiento/permiso del *AUA* permanecerá en efecto hasta que: (1) sea revocada por el padre/madre; (2) el estudiante tenga una cancelación de privilegios de usuario; o (3) el estudiante ya no esté inscrito. Aún sin una firma en el *AUA*, a los empleados, estudiantes, y todos los demás usuarios se les requiere seguir las leyes aplicables, normas, procedimientos, incluyendo los requisitos descritos dentro de este *AUA*. Usando los recursos del distrito, cada usuario está de acuerdo con cumplir con todas las reglas. A cada usuario se le requiere reportar cualquier uso incorrecto de los recursos tecnológicos del distrito al empleado apropiado (ej., maestro, supervisor, u otro personal del distrito). Si el usuario no está seguro acerca de si un uso particular es aceptable o apropiado, él o ella deberán consultar a un maestro, supervisor, u otro personal apropiado del distrito.

Los estudiantes están autorizados para usar los recursos tecnológicos del distrito o equipo para conseguir acceso al Internet u otros servicios en línea en conformidad con la norma de la mesa directiva, las obligaciones del usuario, y responsabilidades especificadas en el *Acuerdo del uso aceptable* del distrito.

Conseguir acceso de recursos tecnológicos fuera de la ubicación de la escuela. Los estudiantes conseguirán acceso a los recursos tecnológicos del distrito fuera de la escuela sólo si un padre/madre o tutor legal supervisa su uso en todo momento. El padre/madre o tutor del estudiante es responsable por monitorear el uso del menor fuera de la escuela.

Consecuencias por el uso impropio

Los estudiantes quienes violen las reglas y el reglamento del distrito o escuela, que incluye los usos inaceptables de los recursos tecnológicos del distrito pueden estar sujetos a consecuencias incluyendo, pero no limitadas a: (1) acción legal; (2) suspensión; (3) expulsión; (3) transferencia a programas alternativos; (4) cancelar o limitar los privilegios de usuario del estudiante; (5) denegación de la participación en las actividades extracurriculares o co-curriculares; (6) u otros privilegios. Cuando un crimen pudo haber sido hecho, el superintendente o designado deberá notificar a las autoridades policíacas locales. De acuerdo con la ley y norma, los estudiantes también pueden estar sujetos a las consecuencias del distrito o escuela, por cualquier conducta fuera del recinto escolar durante las horas que no hay clases que represente una amenaza o peligro para la seguridad de los estudiantes, personal, o propiedad del distrito, o sustancialmente interrumpa las actividades de la escuela.

Denegación de responsabilidad

El distrito no hace garantías y niega cualquier responsabilidad por la exactitud o calidad de la información obtenida usando los recursos tecnológicos del distrito. Cualquier declaración accesible por medio de los recursos del distrito se entiende ser el punto de vista del autor individual y no del distrito, sus afiliados, o empleados. El estudiante y padre/madre/tutor, como condición del uso de los recursos tecnológicos del distrito del estudiante, está de acurdo en indemnizar y librar de cualquier responsabilidad al distrito o a cualquier empleado del distrito y renunciar a todos los reclamos o proceso judicial por daños, costos, o perjuicio surgiendo de la falla de cualquier medida de protección tecnológica, violaciones de restricciones con derechos reservados, errores del usuario o negligencia, u otras obligaciones surgiendo del uso de los recursos tecnológicos del distrito. Cualquier cargo que el usuario acumule debido al uso inapropiado y no autorizado de los recursos del distrito debe ser sostenido por el usuario.

BAKERSFIELD CITY SCHOOL DISTRICT:
ACUERDO DEL USO ACEPTABLE
ACUERDOS ADICIONALES DEL DISTRITO

Seguridad y responsabilidad personal

1. Usaré las computadoras de la escuela sin peligro, responsablemente, y para propósitos educativos.
2. Cuidaré la computadora y todo el equipo de tecnología como si me perteneciera.
3. Mantendré mis contraseñas privadas y no las compartiré con mis amigos.
4. Sólo usaré las computadoras de la escuela para el trabajo del salón de clases asignado por el maestro.
5. Reportaré cualquier mal uso de la computadora o red informática al maestro o al director.
6. Me detendré inmediatamente y le diré al maestro o persona encargada si pasa cualquier cosa en la computadora o en el Internet que está mal, o me hace sentir incómodo.

Usos inapropiados

7. No usaré el nombre de usuario y contraseña de alguien más para entrar a la computadora o red informática.
8. No leeré, borraré, copiaré, o modificaré el correo electrónico o usaré otra identidad de la persona.
9. No intentaré pasar sobre las medidas de seguridad en la red informática del distrito.
10. No bajaré ningún software del Internet a menos que se especifique directamente como parte de la lección.
11. No compraré, venderé, o anunciaré cualquier cosa usando la computadora de la escuela y/o red informática.
12. No usaré el equipo de tecnología para animar el uso de drogas, alcohol, y tabaco o tomar alguna acción que sea poco ética o prohibido por la ley o norma del distrito.

Civismo digital

13. No amenazaré, acosaré, insultaré, burlaré, chismearé, o fastidiaré a otros mientras estoy en línea o usando una computadora. Entiendo que estos comportamientos pueden resultar en castigo que incluye la pérdida de privilegios.
14. No copiaré información y la usaré como si fueran mis propias ideas sin darle crédito al autor de la información y fuente. Sé que la falla de citar apropiadamente mis fuentes de información se le llama plagio y es una forma de hacer trampa.

Comportamiento en línea

15. Entiendo que los archivos de la computadora y comunicaciones electrónicas no son privadas y se puede conseguir acceso por el distrito para asegurar el uso propio.
16. No compartiré información personal (ya sea la mía propia ni de otro estudiante) incluyendo: referencias de donde yo vivo, detalles acerca de la familia o amigos (incluyendo nombres), mi edad, cumpleaños, domicilio, o número de teléfono en el Internet.
17. Usaré un lenguaje respetuoso y apropiado sin decir groserías, insultos, o causar a otros que se sientan incómodos debido a su género, raza, apariencia, comportamiento, o creencias. (Estas son acciones que podrían ser consideradas acoso o intimidación).
18. No publicaré material con derechos reservados en línea.

Firmas requeridas: *Acuerdo del uso aceptable* del BCSD

ESTUDIANTE
Firmando abajo, estoy mostrando que entiendo y estoy de acuerdo en seguir las reglas escritas en este *Acuerdo del uso aceptable* de cuatro páginas. Entiendo que cualquier regla que no siga puede resultar en acción disciplinaria, perder mi cuenta de usuario, y acción legal. Entiendo aún más que puedo ser responsable por usar los recursos tecnológicos fuera de la escuela si mi conducta viola las reglas del distrito. Estoy de acuerdo en reportar cualquier mal uso del sistema electrónico del distrito a un maestro, director, u otro empleado del distrito.

Nombre del estudiante (escribir con letra de molde):_____

Firma del estudiante_____ Fecha_____

PADRE/MADRE O TUTOR
Como el padre/madre/tutor del estudiante, he leído y entiendo este *Acuerdo del uso aceptable* (*AUA*) consistiendo de cuatro páginas. Entiendo que este *AUA* ha sido diseñado para ayudar a asegurar una conducta segura y apropiada mientras que el personal y estudiantes usan los recursos tecnológicos. Firmando abajo, yo consiento a que mi estudiante utilice los recursos tecnológicos del distrito consistente con todas las provisiones de este *AUA*. Entiendo aún más que puedo revocar este consentimiento por escrito, pero esta revocación no afectará ninguna acción tomada en virtud de mi consentimiento antes de que el distrito reciba mi aviso de revocación escrito.

Nombre del padre/madre o tutor (escribir con letra de molde):_____

Firma_____ Fecha_____

MAESTRO PATROCINADOR
He recibido y leído la Norma de la Mesa Directiva 400.43 titulada Uso de tecnología del estudiante, la Adjunta Regla Administrativa, y este *Acuerdo del uso aceptable* (*AUA*) describiendo expectativas para el uso apropiado de los recursos tecnológicos del distrito. Me han proveído con información acerca de la función del personal de supervisar el uso de recursos tecnológicos del estudiante. Como el maestro patrocinador, estoy de acuerdo en instruir al estudiante de cumplir con los requisitos de la norma y del *AUA*. Este compromiso incluye el estar de acuerdo en reportar cualquier uso prohibido o mal uso de los recursos tecnológicos del distrito al administrador apropiado del Distrito Escolar de la Ciudad de Bakersfield y cumplir con todas las leyes, normas, y procedimientos aplicables.

Nombre del maestro/a (escribir con letra de molde):_____

Firma_____ Fecha_____

FOURTH GRADE

Lesson Plan

Connected Culture: The Power of Words

CONNECTED CULTURE

The Power of Words

LESSON PLAN grades 4-5

Essential Question: What should you do when someone uses mean or scary language on the Internet?

Learning Overview and Objectives

Overview: Students consider that while they are enjoying their favorite websites they may encounter messages from other kids that can make them feel angry, hurt, sad, or fearful. They explore ways to handle cyberbullying and how to respond in the face of upsetting language online.

Students discuss all the ways they use technology for communication, put themselves in the shoes of children who are cyberbullied on a kids' game website, and explore both the similarities and differences between in-person versus online communication. Students then brainstorm ways to respond to cyberbullying.

objectives

Students will:

- Empathize with those who have received mean and hurtful messages
- Judge what it means to cross the line from harmless to harmful communication online
- Generate solutions for dealing with cyberbullying

Materials and Preparation

Estimated time: 45 minutes

Materials

- **Words Can Hurt Student Handout**
- **Talk and Take Action Student Handout**
- Colored pencils
- String

Preparation

- Copy the **Words Can Hurt Student Handout**, one for every four students
- Copy the **Talk and Take Action Student Handout**, one for every student
- Cut string the length of the classroom

Parent Resources

- Send parents the **Cyberbullying Parent Tip Sheet**
- Send parents the link to the ***Connected Culture Parent/Teacher Video***

Key Vocabulary

- **Frustrated:** Irritated at not being able to do what you want
- **Cyberbully (verb):** Using technology tools such as the Internet and cell phones to deliberately upset someone else
- **Ethics:** Ideas about how people should act and behave

teaching plans

Introduce

INVITE students to share all the ways they enjoy going online and using digital media, such as cell phones and the Internet.

ASK

- *What are your favorite websites, if any?*
- *What are your favorite video games, if any?*
- *Who do you stay in touch with through cell phones and the Internet?*

ENCOURAGE students to share the positive feelings and experiences they have had with cell phones, the Internet, and other types of digital media.

Teach 1: What's the Problem?

ORGANIZE students into groups of four, and have each group pick a person to record their ideas.

DISTRIBUTE the **Words Can Hurt Student Handout**. Have the groups of students read the scenario about Rani and Aruna receiving mean messages through a children's game website.

HAVE each group answer the questions, and then have them share their responses with the class. Look for responses that show empathy for Rani and Aruna and acknowledge that the messages are mean and hurtful and should be stopped. Ask students to read the "A Matter of Ethics" section on the **Words Can Hurt Student Handout**.

INVITE students to share their own stories.

ASK *Have you seen mean messages sent to you or others online? Tell us about it, but do not use real names.*

PLACE students in pairs. INVITE one partner to write the phrase "You're weird" on a piece of paper, and then hand it to their partner. Tell them that they just received this text.

ASK *What are the reasons the person might have texted "You're weird"?* (They're continuing an inside joke; the first person did something silly at an earlier time; a group of kids is teasing the kid; the person who sent the text really does think the person is weird but is afraid to say it to their face.)

ASK *How did the partner feel who was called weird?* (Possibly like the other person was kidding around, but maybe that the person was teasing or being hurtful.)

Now ask one person from each pair to say to the other person, "You're weird," with a smile on his or her face.

ASK *What are the reasons that the person might have said "You're weird" with a smile on his or her face?* (They're sharing an inside joke; the first person did something silly).

ASK *How did the partner feel who was called weird?* (Like the other person was kidding around, teasing, not serious.)

ASK *Why would you feel differently if you could see the person?* (Look for responses that indicate students understand that people communicate with their faces, bodies, etc.)

Teach 2: Crossing the Line

PLACE the piece of string across the length of the classroom. Ask students to stand on one side of the line. Then ask them to imagine that they are online and somebody has sent them a message, which you will read to them. Tell the students to stay where they are if they think the message is okay; to cross over the line if they think the message is not okay; and to stand *on* the line if they think the message is in between.

READ each of these messages aloud and have students respond:

- *You are an idiot.*
- *I'm having a party and you're not invited.*
- *I like your new haircut.*
- *You are really ugly.*
- *Thanks for the advice. Next time would you mind telling me in person rather than by IM?*
- *Did you finish your homework?*
- *Why is it taking you so long to finish it?*
- *You are such a freak.*

REVIEW with students that kids like to go online and use cell phones to email, chat, watch videos, send messages, play games, and do homework. But sometimes the language can get mean or scary. Messages that make people feel badly cross the line. Sometimes that meanness is unintentional, but when people use tools such as the Internet and cell phones to deliberately upset someone else over and over, that's *cyberbullying*.

Teach 3: Find Solutions

HAVE students return to their seats and refer back to the **Words Can Hurt Student Handout**.

ASK *What could Rani and Aruna do to deal with being cyberbullied?*

EXPLAIN that there are many ways they could choose to solve this problem. Let them know that you will give them ideas about how to handle cyberbullying, but that you think they will come up with great solutions as well.

LEAD a brainstorming session. You may practice brainstorming about an idea unrelated to cyberbullying. For instance, have them first brainstorm about ways that computers can be better used to help students learn. Now invite students to answer the question and think of all the actions that Rani and Aruna could take. Let students know that they should say the first ideas that come to their heads. Tell them they should not be too worried about making mistakes, and that they should not judge others on their responses.

LIST the students' ideas on the board or chart paper. Remind students that they should not pass judgment on other students' ideas at this point.

DISCUSS the entire list with students and decide which solutions are fair to all concerned and respectful of the rights of others.

Teach 4: How to Handle a Bully

COMMEND students for their brainstorming. Let them know if any of the solutions that they suggested had to do with cooling down, finding help or telling a trusted adult, or even ignoring the bully. Explain that these responses are on target, according to information that researchers have gathered about what works when dealing with cyberbullying.

DISCUSS with students how easy it is to feel angry or upset when somebody sends you a mean or scary message online. Explain that cyberbullies deliberately try to make you feel that way, just like real-life bullies deliberately try to make people feel bad. Discuss the following ideas about what they can do when faced with cyberbullying:

- *Cooling down can be a good first step when you receive a mean message online. Taking a deep breath, counting backwards from 10, or pausing to think about what you will do next can give you time to think of the BEST way to handle the situation.*
- *Finding help or telling a trusted adult or a friend can be a good way to take action. You shouldn't deal with the cyberbullying situation alone. The person you tell should be someone who wants to hear what you have to say, and will help you work on a solution. Adults can be especially good because they often have the power to influence the situation, or can give you advice about what to do.*
- *Ignoring the bully can be very effective. Bullies often like attention. When you deprive them of attention, they may lose interest.*
- *Whatever you do, remember to keep a copy of your communication with the bully. If you delete the communication, there is no proof of how the bully treated you if you need to show it to a trusted adult.*

Wrap Up and Assess

You can use these questions to assess your students' understanding of the lesson objectives.

ASK

- *Why is it a bad idea to send mean or scary messages online?* (Because they can make the person who gets them upset, angry, or scared.)
- *Why might there be more misunderstandings between people when they send online messages as opposed to face-to-face discussion?* (Online messages can be more confusing or scarier than face-to-face messages because there are no face-to-face cues to help you understand people's intentions.)
- *What can kids do when they get cyberbullying messages?* (They can (1) calm down and take a deep breath, (2) tell a friend or a trusted adult who can help develop a plan to handle the situation, (3) ignore the bully, (4) keep a copy of the communication with the bully.)

REVIEW with students that words matter and can hurt, and that bullying is not okay – either in the real world or online.

Extension Activity

In small groups, have students make a cyberbully protection kit. The kit should contain a shield that they decorate with an anti-cyberbullying symbol and a scroll that lists things they could say to a cyberbully. The kit can be created with cardboard or paper and markers, or online with Kerpoof (http://www.kerpoof.com).

Homework

Students use the **Talk and Take Action Student Handout** to create a cartoon about a cyberbullying situation. See Make Beliefs Comix for a free online tool: http://www.makebeliefscomix.com. Students create one frame that shows the cyberbullying situation or message. The next frame shows what they might do when faced with this situation or message. The last frame should show a positive outcome of the situation, which might involve confiding in a trusted adult. Encourage students to show their parents their cartoon and to get advice about what they could do. In the final frame, parents provide suggestions about what they might say or do if they learned about the situation.

Alignment with Standards – National Educational Technology Standards for Students© 2007
(Source: International Society for Technology in Education, 2007)

2. Communication and Collaboration
b. communicate information and ideas effectively to multiple audiences using a variety of media and formats

5. Digital Citizenship
a. advocate and practice safe, legal, and responsible use of information and technology
d. exhibit leadership for digital citizenship

Talk and Take Action

STUDENT HANDOUT

grades 4-5

Name _____ **Class** _____ **Date** _____

Directions

Below are three cartoon frames, and directions about what should go in each frame:

FRAME 1: Make a cartoon about something that a cyberbully might do or write online. Remember to use language appropriate for school.

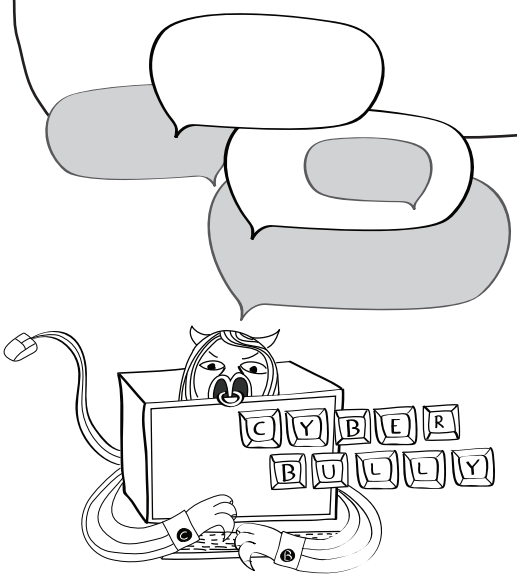
FRAME 2: Show what you might do if you saw what the cyberbully has done or written.

FRAME 3: What might be a positive outcome, or result, of the situation?

You can also use Make Beliefs Comix (http://www.makebeliefscomix.com/) to draw your cartoon online.

What might a cyberbully say or do?

What would you do in response?



What would be a positive outcome?

Use Common Sense!

- If you get upset, take a breather or get offline.
- Tell your parents or another trusted adult when you or someone else is being cyberbullied. Make a plan with the trusted adult about how to respond.
- Ignore and/or block the bully.
- Save a record of the communication between you and the bully.

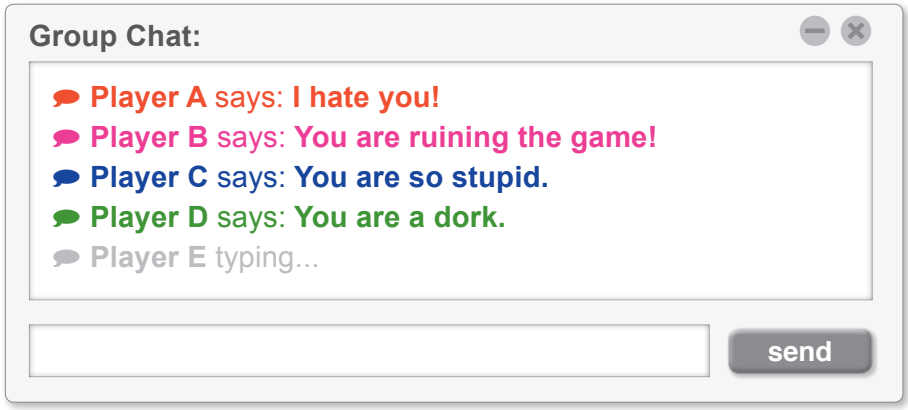
Words Can Hurt

STUDENT HANDOUT grades 4-5

Name(s) _____ **Class** _____ **Date** _____

Directions

Rani and Aruna love a website that has games and chatting for kids. Their parents let them play on the site. Lately, though, Rani and Aruna have been receiving mean messages on the site, including:



Questions:

1. How do you think Rani and Aruna feel when they read those messages?

Rani and Aruna feel _____

_____

2. How would you feel if you received messages like these?

I would feel _____

_____

3. Why do you think people send these kinds of message to people they don't know?

People send these kinds of messages because _____

_____

A Matter of Ethics

There is an old saying that "Sticks and stones may break my bones, but words will never hurt me."

I think that this saying is TRUE/NOT TRUE (circle one) because _____

FIFTH GRADE

Lesson Plan

Safety: Talking Safely Online

SAFETY

Talking Safely Online

LESSON PLAN grades 4-5

Essential Question: What's the difference between Internet friends and real-life, face-to-face pals?

Learning Overview and Objectives

Overview: Students learn that the Internet is a great place to develop rewarding online relationships. But they also learn to be cautious and to never reveal private information to a person they know only online without asking their parent or a trusted adult for permission.

Students discuss the difference between online and real-life friendships, explore an online chat scenario, and complete and sign a checklist for safe online chatting.

objectives

Students will:

- Compare and contrast online friends and real-life, face-to-face pals
- Understand that private information should not be given to anyone online without the permission of a trusted adult
- Learn how to respond if an online friend asks them personal questions

Materials and Preparation

Estimated time: 45 minutes

Materials

- **The Right Answer Student Handout**
- **Chatting Safety Checklist Student Handout**
- Chalkboard or white board

Preparation

- Copy **The Right Answer Student Handout**, one for every student
- Copy the **Chatting Safety Checklist Student Handout**, one for every student

Parent Resources

- Send parents the **Safe Online Talk for Elementary Students Parent Tip Sheet**

Key Vocabulary

- **Uncomfortable:** Anxious; uneasy
- **Monitor (noun):** Someone who closely observes and controls a situation, like a referee
- **Monitor (verb):** To observe closely

teaching plans

Introduce

INVITE students to share their experiences chatting online, instant messaging, and posting on message boards. Explain that sometimes kids might chat online with people they have never met face to face.

CHALLENGE students to explain the differences between messaging with friends they know from school and people they have never met face to face.

EXPLAIN that kids sometimes have what seems to be a close relationship with an online friend, but they cannot possibly know a person online as well as they know a face-to-face friend.

ASK *Can you ever really know if an online-only friend is male or female?*

ASK *Can you know for sure how old an online-only friend is?*

EXPLAIN that the answer is NO – you can't know for sure. So kids should talk to online friends with caution, and not reveal personal information that could put them in danger in any way. Never give online-only friends private information about yourself, such as your address or phone number, without first asking permission from a parent or guardian.

Teach 1: You're in Charge

DISTRIBUTE The Right Answer Student Handout.

HAVE students read the scenario about Sita and CJcool11 and then answer the handout questions individually. Note that they will refer back to this handout in Teach 4.

Teach 2: Friends and Strangers

ASK *Why may it be easier to share school problems with an online friend than a real-life, face-to-face pal?* (It may be easier because online-only friends are not from school, so they might be able to see both sides of an issue, and they don't have to worry about what the other kids in school will think.)

REMIND students that they can't know for sure that an online friend is really a kid or someone they can trust. Make sure they know it's easy to hide your real identity when you're online.

ASK *Have you ever pretended to be someone you are not? If so, when?* (Answers may include Halloween, school plays, jokes.)

EXPLAIN to students that online friends might sometimes pretend too. They might not really be who you think they are. That's why it's important to never share private information about yourself with online friends without asking your parent or guardian first. You wouldn't give private information to a stranger without asking, and it's important to treat online friends the same way. (If students ask why, you can explain: *There are criminals who trick people into giving out private information about others. Then they use that private information to pretend to be them. They might even pretend to be them in order to steal their money. This is called identity theft. Giving out certain pieces of information to strangers can also let them know where you are located. This could be dangerous.*)

NOTE: The latest research indicates that pre-adolescent children are generally not the targets of online predators, and that the news media-driven idea that predators piece together private identity information to abduct a child is not supported. In this lesson we discuss the safety risks associated with giving out our personal information online, but we also address the risk of identity theft. It is never too early for children to learn about identity theft. Children are often targeted because they usually have clean credit histories and their parents are unlikely to be alert for signs that someone is using their child's identity. Children who learn about identity theft can also help protect their parents' identities online.

Teach 3: Stay Safe

ASK *What's private information?* (Answers may include address, phone number, passwords, etc.)

EXPLAIN that private information includes (write the following on the board):

- full name
- street address
- name of school
- school address
- email address
- phone numbers
- passwords
- calling card number
- mother's maiden name
- parent's place of work
- photos in which you can be recognized

REMIND students that if an online friend asks for any of that information, they should tell a trusted adult.

DISCUSS with students that the best way to talk safely to online friends is on a website that's just for kids. Most of these sites have adult monitors that check the chat and messaging. A monitor is like a referee at a game. Monitors keep track of the chat to make sure that everyone keeps the chat on topic, uses good manners, and stays safe.

Teach 4: Check it Out

DISTRIBUTE the **Chatting Safety Checklist Student Handout**.

HAVE students read, discuss, complete, and sign the checklist.

HAVE students revisit their responses to **The Right Answer Student Handout**.

ASK *Would you change your advice to Sita? If so, how?*

DISCUSS possible answers with students. Point out that Sita and CJcool11 are online friends, not real-life, face-to-face pals. It is okay to talk with online friends. You can have very good talks with them, and share ideas and

feelings that you might not share with friends at school. But you should never share private information aboutyourself without first asking your parent or a trusted adult, and you shouldn't answer questions that make you feel uncomfortable.

EXPLAIN that when Sita's online friend asks her "Where is your school?" she could answer, "I'd rather not say," or "That's private. Let's not go there." Point out that Sita doesn't have to answer at all. She can just log out of the messaging service or website, or block the person who is asking the questions.

REMIND kids that when people persist in asking any question that makes them feel uncomfortable, they can ask a trusted adult to help them report these people to the website owners.

Wrap Up and Assess

You can use these questions to assess your students' understanding of the lesson objectives.

ASK

- *How are online friends and real-life, face-to-face friends different?* (Even when you share personal thoughts with an online friend, this person is as much a stranger as someone you meet on the street for the first time. You know face-to-face friends much better. Just seeing them in school or around your neighborhood gives you a lot of information about them.)
- *What should you do when an online friend asks for private information?* (Never give out private information without first asking the permission of a parent or guardian.)

REVIEW with students that they can have rewarding chats with online friends, but they should be as careful with online friends as they are with real-life strangers.

Extension Activity

Have kids find kid-friendly websites that have monitors in their chat areas. Ask them to visit three of these websites and observe the chatting that is occurring. Ask them to reflect on whether anyone is revealing personal information. They should report back to the class and think about ways websites could teach kids not to reveal this information.

Alignment with Standards – National Educational Technology Standards for Students© 2007
(Source: International Society for Technology in Education, 2007)

2. Communication and Collaboration
b. communicate information and ideas effectively to multiple audiences using a variety of media and formats

5. Digital Citizenship
a. advocate and practice safe, legal, and responsible use of information and technology

Chatting Safety Checklist

STUDENT HANDOUT grades 4-5

Name _____ **Class** _____ **Date** _____

You're ready to chat or talk with others online when you can check that each statement about you is true.

- ☐ My parents say it's okay for me to chat and message online.
- ☐ I will only chat and message on kids' websites that have monitors – people who review what is being said.
- ☐ I will check in with a trusted adult before replying to, clicking on a link from, or IMing someone who is not a face-to-face friend.
- ☐ I will pick chat and messaging screen names that do not include private identity information.
- ☐ I know what kinds of information are private.
- ☐ I will not give out private information when talking online.
- ☐ I will not answer questions that make me uncomfortable.
- ☐ I will leave the site and tell a trusted adult if someone bothers me online.
- ☐ I will never meet someone in person who I first met online without bringing a parent or guardian with me.

Signature _____ Date _____

Use Common Sense!

Remember not to share these types of private information:

- Full name
- Street address
- Name of school
- School address
- Email address
- Phone numbers
- Passwords
- Cell phone number
- Mother's maiden name
- Parent's place of work
- Photos in which you can be recognized

The Right Answer

STUDENT HANDOUT grades 4-5

Name **Class** **Date**

Sita likes to visit a website where kids can post messages about school, their favorite TV shows, and current events. She really likes the kid who uses the screen name CJcool11. When Sita shares a problem she has at school, CJcool11 always has good ideas for handling the problem. Even though she has never met CJcool11 in person, Sita thinks of CJcool11 as a friend.

One day, while messaging, CJcool11 and Sita compare their two schools.

Sita types, "My school principal is so strict. We have to walk through the halls in straight lines!"

CJcool11 answers, "My school isn't so strict. What's the name of your school?"

This question gives Sita a bad feeling. Sita feels uncomfortable about giving that information to CJcool11.

She types back, "Uh, my school's name is too hard to spell."

CJcool11 types, "So where is your school?"

Why do you think Sita gets a bad feeling when CJcool11 asks for the name of her school?

What should Sita answer?

What makes this answer a good one?

Use Common Sense!

If things get creepy or uncomfortable when you're chatting online, take action.

- Log out of the website or messaging service
- Tell a parent or trusted adult
- Ignore the person, or block that person from chatting with you